

SYSTEM AND METHOD OF OPERATING SYSTEM IDENTIFICATION

Beddoe et al.

Appl. No.: Unknown Atty Docket: FNDSTN.032A

1 / 4

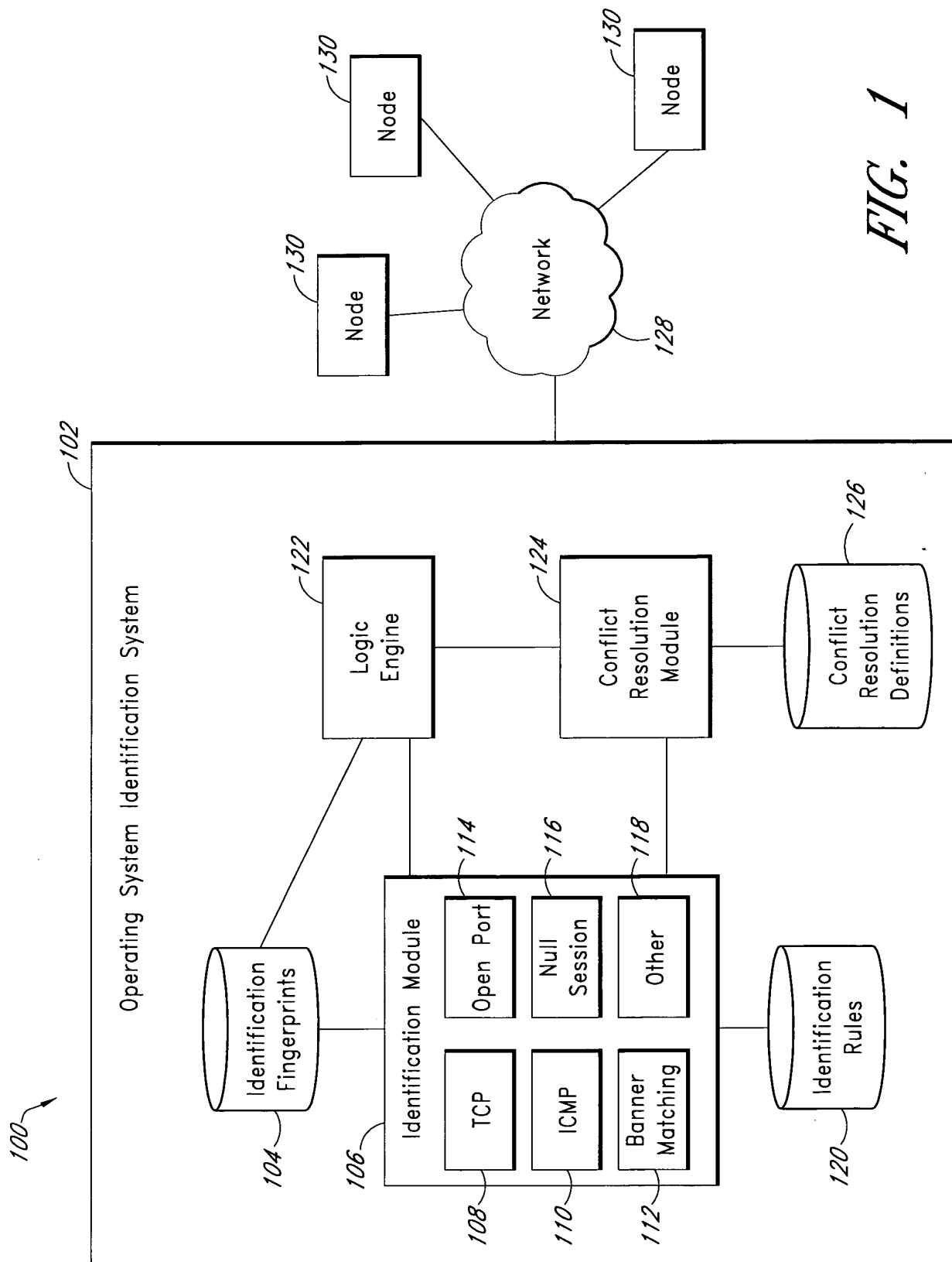
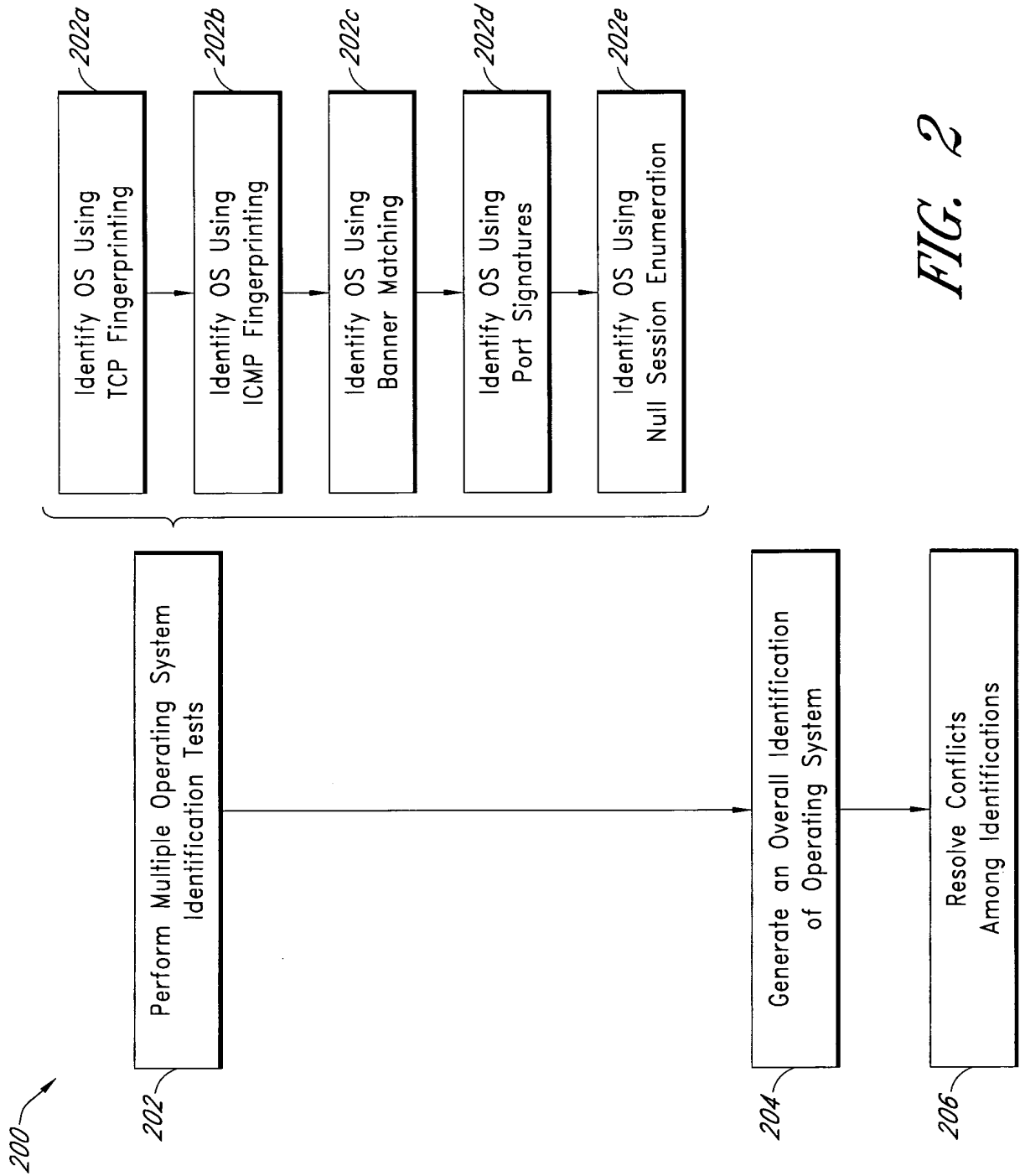


FIG. 1



300

Identification Conflicts				
TCP		ICMP	Banner Matching	Open Port
Windows XP (95%)		Unix (80%)	Windows XP (90%)	Windows 98 (60%)
Mac OS (75%)		Unix (95%)	Windows 95 (40%)	Unix (80%)
Mac OS (90%)		Windows XP (80%)	Mac OS (95%)	Mac OS (80%)
				Null Session
				Windows XP (100%)
				N/A
				N/A

FIG. 3

400
Conflict Resolution Definitions

402	404	406	408	410	412	414	416
TCP Fingerprint	ICMP Fingerprint	TCP Ports	UDP Ports	TCP Port & Banner	UDP Port & Banner	OS Description	OS Code
T40E8:4100:4080: 0586:0:80:0001:1:0: MNWNNTNS	I0001303	139, -445	137	—	—	Windows 2000	OS_Win2000
T8000:80BC:8154: 05B4:0:40:0001:1:1: MNWNNT	I00017913	—	—	—	—	OS X	OS_MAC
T2000:2000:2000: 05B4:0:40:0001:0:0: MNW	I00137993	—	—	—	—	Xerox Phaser 7300	OS_PRINTER
T4000:4100:4080: 05B4:4:40:0001:1:1: MNWNNT	I0013793	—	—	—	161: BIG/ip	FreeBSD	OS_BSD

FIG. 4